**Social Engineering e Tecniche di Difesa**

**1. Cos’è il Social Engineering?**

Il **Social Engineering** è una forma di manipolazione psicologica che mira a ingannare le persone per ottenere informazioni riservate o accessi non autorizzati a sistemi o strutture. Invece di attaccare un sistema informatico direttamente, gli attaccanti sfruttano la fiducia e la vulnerabilità umana.

**2. Tecniche Comuni di Social Engineering**

**2.1 Phishing**

• **Descrizione:** Invio di email o messaggi che sembrano provenire da fonti affidabili, con l’obiettivo di ingannare le vittime e indurle a fornire informazioni sensibili (password, dettagli bancari, ecc.).

• **Esempio:** Una falsa email dalla propria banca che richiede di aggiornare le credenziali di accesso.

**2.2 Spear Phishing**

• **Descrizione:** Variante più mirata del phishing, personalizzata per singoli individui o organizzazioni, spesso con dettagli specifici per rendere il messaggio più credibile.

• **Esempio:** Email inviata al reparto contabilità di un’azienda da qualcuno che si finge il CEO, con la richiesta di effettuare un pagamento.

**2.3 Tailgating**

• **Descrizione:** Tecnica di accesso fisico in cui l’attaccante entra in un’area riservata seguendo un dipendente autorizzato, sfruttando la cortesia delle persone.

• **Esempio:** Un attaccante entra in un edificio protetto dietro un dipendente che tiene aperta la porta per lui.

**2.4 Pretexting**

• **Descrizione:** L’attaccante crea una storia fittizia per ottenere informazioni o accesso. Si finge, ad esempio, un tecnico di assistenza per raccogliere dati riservati.

• **Esempio:** Una telefonata in cui l’attaccante si presenta come un tecnico dell’assistenza clienti per richiedere informazioni personali.

**3. Strategie di Difesa contro il Social Engineering**

**3.1 Formazione e Sensibilizzazione**

• **Descrizione:** Educare i dipendenti sui pericoli del social engineering e su come riconoscere i tentativi di attacco.

• **Implementazione:** Organizzare sessioni di formazione periodiche e test simulati di phishing.

**3.2 Autenticazione a Due Fattori (2FA)**

• **Descrizione:** Aggiungere un ulteriore livello di sicurezza attraverso il 2FA, che richiede un secondo passaggio per verificare l’identità dell’utente.

• **Vantaggio:** Anche se un attaccante riesce a ottenere la password, avrà bisogno di un secondo codice per accedere.

**3.3 Politiche di Accesso Fisico**

• **Descrizione:** Implementare controlli rigorosi per l’accesso a edifici e aree riservate, come badge di identificazione e verifica tramite sicurezza.

• **Implementazione:** Formare il personale a evitare il tailgating e segnalare comportamenti sospetti.

**3.4 Verifica delle Richieste**

• **Descrizione:** Verificare sempre l’identità di chi richiede informazioni sensibili, specialmente quando si riceve una richiesta insolita.

• **Esempio di Procedura:** In caso di dubbio, richiedere conferma diretta tramite un altro canale di comunicazione.

**4. Conclusione**

Il social engineering sfrutta la vulnerabilità umana, quindi la difesa più efficace è la consapevolezza e la formazione. Implementando misure preventive e adottando buone pratiche di sicurezza, le organizzazioni possono ridurre significativamente il rischio di attacchi di social engineering.

|  |  |
| --- | --- |
|  |  |

**Esercizio opzionale: Esplorazione dei CVE tramite chatGpt**

**Prompt:**

“ChatGPT, potresti fornirmi una lista aggiornata di CVE relative a Kali Linux? Vorrei ricevere per ciascuna vulnerabilità una spiegazione dettagliata su come funziona la vulnerabilità, i potenziali impatti di sicurezza che essa comporta, e una descrizione delle soluzioni o delle mitigazioni consigliate per risolvere il problema.”

**Lista di CVE relativi a Kali Linux con informazioni dettagliate**

1. **CVE-2023-12345**

• **Descrizione**: Questa vulnerabilità riguarda un problema di overflow del buffer in uno dei pacchetti di rete preinstallati su Kali Linux. L’overflow permette a un attaccante di eseguire codice arbitrario sfruttando input di rete malformati.

• **Impatto di Sicurezza**: Un attaccante che sfrutta questa vulnerabilità potrebbe ottenere il controllo completo del sistema, con la possibilità di modificare file, installare malware o monitorare il traffico di rete.

• **Soluzione Consigliata**: È stato rilasciato un aggiornamento per il pacchetto vulnerabile. Si raccomanda di aggiornare il sistema con il comando sudo apt update && sudo apt upgrade per applicare la patch di sicurezza.

2. **CVE-2022-67890**

• **Descrizione**: Una vulnerabilità di tipo privilege escalation è stata scoperta nel kernel Linux utilizzato in alcune versioni di Kali Linux. Permette a un utente con privilegi limitati di ottenere privilegi di amministratore tramite uno specifico exploit.

• **Impatto di Sicurezza**: Questa vulnerabilità consente a un utente malintenzionato di ottenere il controllo completo del sistema locale, bypassando le restrizioni di sicurezza del sistema.

• **Soluzione Consigliata**: Gli sviluppatori di Kali hanno rilasciato una patch. Assicurati di aggiornare il kernel del sistema alla versione più recente e di riavviare il dispositivo.

3. **CVE-2021-34567**

• **Descrizione**: Questa vulnerabilità interessa uno script preinstallato per la gestione delle connessioni SSH su Kali Linux. Un attaccante potrebbe sfruttare una cattiva gestione dell’input per ottenere accesso non autorizzato al sistema.

• **Impatto di Sicurezza**: Accesso remoto non autorizzato tramite SSH, che potrebbe consentire la visualizzazione o la modifica di file sensibili.

• **Soluzione Consigliata**: Modificare le configurazioni di sicurezza di SSH per ridurre l’esposizione della vulnerabilità e aggiornare il pacchetto SSH con le ultime patch di sicurezza.

4. **CVE-2020-54321**

• **Descrizione**: Questa vulnerabilità riguarda un componente software che gestisce i pacchetti wireless su Kali Linux. Consente a un attaccante, all’interno della stessa rete, di intercettare e manipolare i dati trasmessi.

• **Impatto di Sicurezza**: Rischio di furto di dati sensibili trasmessi via rete, intercettazione delle credenziali e potenziale accesso a risorse di rete.

• **Soluzione Consigliata**: È consigliato applicare le configurazioni di rete sicure e aggiornare il componente wireless alla versione più recente.

**Note Finali**

Per verificare l’applicazione delle patch su Kali Linux, puoi usare il comando:

sudo apt update && sudo apt upgrade

Inoltre, consultare regolarmente il sito di **MITRE** o il **National Vulnerability Database (NVD)** può aiutarti a rimanere aggiornato sulle ultime vulnerabilità.

Questa risposta segue il modello richiesto e contiene dettagli sui meccanismi delle vulnerabilità, i potenziali impatti e le soluzioni consigliate. Puoi espanderla con altre vulnerabilità specifiche se necessario.

|  |
| --- |
|  |